

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Google accounts csikirby@gmail.com,
csikirby82@gmail.com, becauseiamawesome82@
gmail.com, and sekirby2@gmail.com

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A-1located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

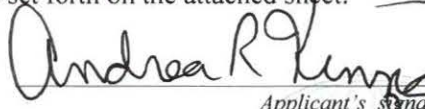
Code Section

See Attachment C-1

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date:

7-18-19

City and state: Dayton, Ohio


Judge's signature
Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-1

Information associated with the Google accounts csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, and sekirby2@gmail.com that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B-1
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

Email Accounts:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service utilized;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

Google Photo Accounts:

6. Subscriber registration information;
7. All photographs and videos currently or previously contained in the user’s account or shared albums, to include deleted photographs and videos, and any associated file information;

Google Drive Accounts:

8. Subscriber registration information;
9. Any files created or previously contained in the user’s account, to include deleted files, and any associated file information;
10. Any IP logs and other information associated with files from the account;

Web and App History:

11. Subscriber and registration information;
12. Any available Web and App History data;
13. Any IP logs associated with the Web and App History Data;

Google+:

14. Subscriber registration information;
15. Circle information to include name of Circle and members, contents of postings, comments, photographs, and time stamps;
16. Community information, to include name of Community and members, contents of Communities, and comments;
17. Hangout information, to include name of Hangouts and any preserved videos;
18. Any photographs and videos posted on the user's account and associated comments;
19. Any comments posted to other users' accounts.

Android Backup:

20. Any available backup data for any electronic devices.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), from April 23, 2018 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.
2. Any visual depictions of minors.
3. Any Internet or search history indicative of searching for child pornography or content involving children.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors.
6. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
7. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
8. Any information related to the use of aliases.
9. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.
10. Any invoices or receipts for hotel stays.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-1

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt, Distribution, Attempted Receipt, and Attempted Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt, Distribution, Attempted Receipt, and Attempted Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents and investigators of the Homeland Security Investigations (HSI) and FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by STEPHEN E. KIRBY II (hereinafter referred to as "KIRBY"). As further detailed below, the investigation has determined that KIRBY has utilized the account names of "mymister2018", "yourmister2018", and "yourmister2019" on a smartphone instant messenger application; namely, the Kik Messenger application. This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Information associated with the Google accounts csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, and sekirby2@gmail.com that is stored at premises controlled by Google LLC (as more fully described in Attachment A-1); and
 - b. Information associated with the Microsoft OneDrive accounts associated with the email addresses csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, sekirby2@gmail.com, and riversidepresident2006@yahoo.com that is stored at premises controlled by Microsoft Corporation (as more fully described in Attachment A-2).
3. The purpose of the Applications is to seize evidence of the following violations:
 - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography; and
 - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce.
4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and are incorporated by reference.
5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the

investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 and A-2).
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present in the information associated with the above noted accounts (as described in Attachments A-1 and A-2).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
10. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
11. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting

interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

12. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:
 - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).
 - e. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is

192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- f. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- g. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- h. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

Collectors of Child Pornography

- 14. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce,

convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Google Services

- 15. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.
- 16. Google Photos is a photograph and video sharing and storage service provided by Google LLC, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.
- 17. Google+ is a social networking and identity service website owned and operated by Google LLC, located at www.plus.google.com. Common features include the following:
 - a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.

- b. Circles: Google+ allows users to establish “circles”, which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical “Friends” list function used by sites such as Facebook and MySpace.
 - c. Communities: Communities allow users with common interests to communicate with each other.
 - d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.
 - e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.
 - f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.
18. Google Web and App History is a feature of Google Search in which a user’s search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user’s Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.
19. Google Drive is a file storage and synchronization service provided by Google LLC, located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.
20. Google Android Backup is a service provided by Google LLC to backup data connected to users’ Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users’ devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

Email Accounts

21. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the accounts listed in Attachment A-1. Subscribers obtain accounts by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.
22. In general, emails that are sent to Google LLC subscribers are stored in the subscriber’s “mail box” on Google LLC’s servers until the subscriber deletes the email. If the subscriber does not

delete the message, the messages can remain on Google LLC's servers indefinitely. Even if the subscriber deletes an email, it may continue to be available on Google LLC's servers for a certain period of time.

23. Google LLC subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
24. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.
25. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
26. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
27. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia

of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Microsoft OneDrive

28. Microsoft Corporation is a company based in Redmond, Washington. Microsoft Corporation provides a variety of online services to the public, including an online storage service called OneDrive (formerly known as SkyDrive). OneDrive is an Internet-based storage medium that can be accessed from computers and other electronic storage devices, such as cellular telephones and tablets. OneDrive allows users to store files on Microsoft’s servers and access the files from any of their devices that are connected to the Internet.
29. When a user transfers a file to a OneDrive account, it is initiated at the user’s computer, cellular telephone, or tablet and transferred via the Internet to Microsoft’s servers. The file is then automatically synchronized and transmitted to other computers or electronic devices that have been registered with that OneDrive account and to Microsoft’s servers. If the subscriber does not delete the contents of his/her account, the files can remain on Microsoft’s servers indefinitely. Even if the subscriber deletes his/her account, it may continue to be available on Microsoft’s servers for a certain period of time.
30. OneDrive allows subscribers to obtain accounts at the domain name www.onedrive.live.com. Subscribers obtain a OneDrive account by registering with an email address. During the registration process, OneDrive asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers, other identifiers, alternate email addresses, and (for paying customers) means and source of payment.
31. Online storage providers such as OneDrive typically retain certain transactional information about the creation and use of a subscriber’s account on their system. This information can include the date on which the account was created, the length of service, records of log-in times and durations, the types of services utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files

that reflect usage of the account. In addition, online storage providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account and the locations where the account was accessed.

32. In some cases, OneDrive account users will communicate directly with Microsoft about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

Kik Messenger Application

33. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
34. The Kik messenger application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
35. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. Kik Interactive Inc. does not verify this information, and as such, users can provide inaccurate information.
36. Kik Interactive Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, Kik Interactive Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. Kik Interactive Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). Kik Interactive Inc. does not store or maintain chat message content.
37. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.
38. Kik Interactive Inc. has developed procedures to monitor and identify Kik accounts that may be utilized to commit child pornography and/or child abuse offenses. Kik Interactive Inc. typically reports any accounts that are identified to the Royal Canadian Mounted Police. The Royal Canadian Mounted Police typically refers information about any accounts that appear to utilize Internet service in the United States to agents of the Homeland Security Investigations

(HSI).

Telegram Messenger

39. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.
40. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.
41. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chats on Telegram's servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires.
42. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis.
43. Based on my training and experience, I know that individuals involved in child pornography and child abuse offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

Omegle

44. Omegle is a free online chat website located at www.omegle.com. The website is administered by Omegle.com LLC, a company based in Spokane, Washington. The website allows users to communicate with each other anonymously. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names "You" and "Stranger".
45. Omegle was initially a text-only chat program. In 2010, Omegle introduced a video mode to complement the text chat mode, which paired together users with web cameras and microphones. Additional features have been added over the years. One such feature is the option to input "interest" tags. Adding interests lets users to be paired together who have something in common with each other.
46. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Omegle application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Omegle application provides an anonymous means of trading child pornography and communicating about the sexual abuse of children.

Cloud Storage

47. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
- a. “Cloud” is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. “The cloud” was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.
 - b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
 - c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.
48. Dropbox is an on-line file hosting service operated by Dropbox Inc., a company headquartered in San Francisco, California. Dropbox accounts provide users with cloud storage, file synchronization, personal cloud, and client software. Dropbox creates a special folder on the user’s computer, and the contents of the folder are synchronized to Dropbox Inc.’s servers and to other computers and devices onto which the user has installed Dropbox, keeping the same

files up-to-date on all devices. Users are provided 2 GB of free storage space for basic accounts.

49. Mega is a cloud storage and file hosting service offered by Mega Limited, an Auckland-based company. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.
50. Dropbox and Mega provide its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a “sharing link”. A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.
51. Based on my training and experience, I know that individuals with large collections of child pornography files may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement. Furthermore, individuals often utilize sharing links to their cloud storage accounts to share child pornography files with others.

Virtual Private Networks

52. A Virtual Private Network, commonly known as a VPN, provides programming that creates a safe and encrypted connection over a less secure network, such as the public Internet. A VPN works by using a shared public infrastructure while maintaining privacy through security procedures and tunneling protocols.
53. A VPN extends a private network across a public network, and it enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device (such as a laptop, desktop computer, or smartphone) across a VPN may benefit from the functionality, security, and management of the private network. Encryption is a common though not inherent part of a VPN connection. A number of Electronic Service Providers offer VPN's to customers worldwide.
54. An inherent benefit of a VPN is the ability to conceal one's browsing activity. Based on my training and experience, I know that individuals involved in child pornography offenses and other illegal activities sometimes use VPN's to conceal their activities from law enforcement.

GigaTribe

55. GigaTribe is a freeware program that allows users to create their own private Peer-to-Peer network of contacts. To use GigaTribe, users download the free program and then select which folder(s) on their computer they want to share. Users do not automatically share files when using GigaTribe. File sharing is limited only to other users who have been added to one's

private network via a “friends” request. Acceptance of a friend request permits that user to access and download files from the initiator of the request only, and vice versa; therefore each user is his/her own network administrator.

56. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize Gigatribe and other Peer-to-Peer applications to obtain and share child pornography files.

Cellular Telephone Data

57. Sprint Corporation and Verizon are companies that provide cellular telephone access to the general public. I know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.
58. Based on my training and experience, I know that Sprint Corporation and Verizon can collect cell-site data about cellular telephones. I also know that Sprint Corporation collects Per Call Measurement Data (PCMD), and Verizon collects Range to Tower (RTT) data. Both PCMD and RTT data capture the time it takes for a signal to travel from the tower to the handset and back again. Based on this time, the network will provide a distance between the tower and cell phone. Furthermore, I know that wireless providers such as Sprint Corporation and Verizon typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

Common Abbreviations

59. Based on my training and experience, I know that individuals frequently use abbreviations or acronyms when communicating with each other on messenger applications such as Kik and Telegram. Some of these abbreviations or acronyms include the following (as seen later in the Affidavit):
- a. Dau – Daughter
 - b. Diff - Different
 - c. Gf – Girlfriend
 - d. Lol – Laugh out loud
 - e. Perv – Pervert
 - f. Ppl – People
 - g. U – You

- h. Ur – Your
- i. Vid – Video
- j. Yng - Young
- k. YO – Years old

FACTS SUPPORTING PROBABLE CAUSE

Background Information of KIRBY

- 60. During the 2011 through 2013 time period, the FBI and Moraine (Ohio) Police Department investigated KIRBY for child pornography offenses. The investigation determined that KIRBY utilized the Gigatribe Peer-to-Peer file sharing program to trade child pornography files with others, and that he utilized both the Gigatribe Peer-to-Peer file sharing program and the Yahoo Messenger application to discuss the sexual exploitation and sexual abuse of children with various other users. As part of the investigation, a search warrant was executed at KIRBY's residence in Moraine, Ohio. Over 16,000 images and over 300 videos of child pornography were recovered from KIRBY's electronic devices that were seized pursuant to the warrant.
- 61. On or around May 7, 2012, KIRBY was arrested pursuant to a federal arrest warrant for one count of possession of child pornography (in violation of 18 U.S.C. § 2252(a)(4)(B)) and one count of distribution of child pornography (in violation of 18 U.S.C. § 2252(a)(2) and (b)). On or around May 17, 2013, KIRBY pled guilty to one count of distribution of child pornography. On or around November 13, 2013, KIRBY was sentenced to 60 months imprisonment and five years of supervised release.
- 62. KIRBY was released from prison and entered a halfway house on or around January 9, 2018. On or around April 23, 2018, KIRBY was released from the Bureau of Prisons' custody and began his five-year term of supervised release. He is currently supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in Dayton, Ohio. As part of the conditions of his supervised release, KIRBY is prohibited from possessing or using any computer or device with access to any on-line computer service at any location without prior written approval of his probation officer. PO Owens authorized KIRBY to utilize the email account sekirby2@gmail.com to search for jobs, provided that KIRBY only accessed the account from a public library. Otherwise, KIRBY is prohibited from having any electronic accounts or accessing Internet data from his cellular telephone or any other electronic devices.
- 63. KIRBY has reported to PO Owens that since he was released from the Bureau of Prisons' custody, he has lived with his grandmother (who will be referred to for purposes of this Affidavit as "Adult Female A") at 5068 Nielson Court, Huber Heights, Ohio (hereinafter referred to as the "SUBJECT PREMISES"). Pursuant to the terms of KIRBY's supervised release, PO Owens has conducted multiple home visits at the SUBJECT PREMISES. PO Owens typically notified KIRBY in advance of the dates and times of these home visits.
- 64. KIRBY has also reported to PO Owens that he utilizes an iPhone bearing telephone number 937-684-5792 (hereinafter referred to as "TARGET CELL PHONE-2"). PO Owens has authorized KIRBY to utilize this device, provided that the Internet browser is disabled. Again pursuant to the terms of KIRBY's supervised release, PO Owens has regularly reviewed the contents of TARGET CELL PHONE-2. PO Owens has not observed any child pornography

files, evidence of utilization of an Internet browser, or evidence of utilization of messenger applications on this device. PO Owens has also reviewed the contents of the sekirby2@gmail.com email account. PO Owens has not observed any child pornography files in this email account.

65. As part of his conviction, KIRBY is required to register as a sex offender. KIRBY completed his registration paperwork on or around April 24, 2018, and he renewed the registration paperwork on or around May 21, 2018 and November 13, 2018. On the paperwork for the initial registration and two renewals, KIRBY identified that he resided at the SUBJECT PREMISES. As part of his registration renewal on or around November 13, 2018, KIRBY reported that he worked at a business in Vandalia, Ohio.
66. As part of the investigation (and as further detailed below in paragraphs 95 through 98), surveillance was conducted of KIRBY on several occasions. The surveillance activities identified that KIRBY drove a 2015 Nissan Altima bearing Ohio license plate 661 YTM (hereinafter referred to as the "SUBJECT VEHICLE").
67. Records from the Ohio Bureau of Motor Vehicles identified that KIRBY utilizes the SUBJECT PREMISES on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles also identified that the SUBJECT VEHICLE is presently registered to KIRBY's father, STEPHEN KIRBY I. Records from the Montgomery County (Ohio) Auditor's website identified that the SUBJECT PREMISES is presently owned by Adult Female A and KIRBY's grandfather. KIRBY's grandfather is deceased.

Account Identified by Kik Interactive Inc.

68. In or around June 2018, as part of its ongoing monitoring of accounts (as detailed above in paragraph 38), Kik Interactive Inc. identified that a Kik account with an account name of mymister2018 was involved in a group chat that may have discussed child pornography and/or child abuse material. Excerpts from this group chat, as well as subscriber information for the mymister2018 Kik account, was provided to the Royal Canadian Mounted Police. After determining that the mymister2018 Kik account appeared to utilize Internet service in the United States, the Royal Canadian Mounted Police turned over the information to HSI agents. In April 2019, I obtained these records from HSI.
69. Based on the records provided by Kik Interactive Inc., the name of the group chat that the mymister2018 account user participated in was "Bi,Gay boys for Daddys(18?+ only)". Also based on records provided by Kik Interactive Inc., the group chat occurred on or around June 8, 2018. It appeared that Kik Interactive Inc. only provided small excerpts of this chat. These excerpts included the following:

mymister2018:	Had a boss used to tell me all about her sons puberty and erections. He was hot too <Conversation Break>
Kik User 2:	U have link DropBox and Mega?
Kik User 2:	Lots of stuff if you d <Conversation Break>
mymister2018:	Post in here

Kik User 2: *Submits URL containing apparent sharing link to a
Dropbox account.*
<Conversation Break>
Kik User 2: Send me link please
mymister2018: Let me get into my email that has them all.

70. Based on my training and experience, I know that individuals involved in child pornography offenses often trade child pornography files by exchanging sharing links to files in their cloud storage accounts. I also know that child pornography offenders sometimes store lists of their sharing links in Word files, Text files, and draft email messages.
71. Based on the comment made by the mymister2018 account user about a boy experiencing puberty, it appeared that the Kik users in the above noted group chat were discussing children. Based on the contents of the conversation as well as other information detailed in the Affidavit (including information detailed below), it is reasonable to believe that the Dropbox link posted by Kik User-2 may possibly have contained child pornography or child erotica files. It is also reasonable to believe that the user of the mymister2018 Kik account had an email account that he/she might have utilized to store sharing links to files in his/her cloud storage account(s), possibly to include child pornography and/or child erotica files.

FBI Undercover Investigation – Kik Platform, December 2018 to January 2019

72. In December 2018 and January 2019, agents and task force officers of the Washington, D.C. Field Office of the FBI were involved in an ongoing online investigation to identify individuals utilizing social media and texting applications to commit child exploitation offenses. As part of the investigation, an undercover officer who will be referred to for purposes of this Affidavit as “UCO-1” routinely chatted with individuals who UCO-1 met on various social media applications.
73. On or around December 29, 2018 and January 2, 2019, UCO-1 chatted via Kik Messenger with a Kik account user utilizing the account name of yourmister2018. Below is a summary of this chat:
- a. The yourmister2018 account user indicated that he was 36 years old, was from Ohio, and had children who were 15 years old, 14 years old, and six years old.
 - i. I know that KIRBY was 36 years old at the time of this chat. I have also determined that KIRBY has two biological children who were approximately 15 years old and 14 years old at the time of the chat. I have also determined that KIRBY’s ex-wife (who will be referred to for purposes of this Affidavit as “Adult Female B”) has another son who was approximately six years old at the time of the chat.
 - b. UCO-1 purported that he engaged in sexual activities with his children, and he inquired if the yourmister2018 account user did the same. The yourmister2018 account user responded by stating: “Working on the 6 yo. Active some with a 10 and diff 6 yo. Was active with my teens when they were 2-5 but stopped. Got several other teens thiugh. You got videos of you”.

- i. Based on this response and the context of the conversation, it appeared that the yourmister2018 account user was indicating that he engaged in sexual activities with children. It also appeared that the yourmister2018 account user was soliciting UCO-1 for videos of UCO-1 engaging in sexual activities with his children.
- c. The yourmister2018 account user inquired about Telegram groups of which UCO-1 was aware.
- d. The yourmister2018 account user stopped communicating with UCO-1 on or around December 29, 2018, after stating that he was “out in public”. UCO-1 re-initiated the conversation on or around January 2, 2019 and called the yourmister2018 account user “fake”. The yourmister2018 account user responded by stating “Nah just don’t trade my shot for free”.
- i. Based on my training and experience, I know that individuals involved in trading child pornography files often have quid pro quo relationships with their trading partners, and they often will not send files to others until they receive child pornography files from their trading partners. The above noted statement by the yourmister2018 account user is consistent with this practice. The statement is also consistent with someone who has access to child pornography files.

Information Provided by Cooperating Witness

- 74. In February 2019, an adult male who will be referred to for purposes of this Affidavit as “Adult Male A” reported to the Huber Heights (Ohio) Police Department that a person by the name of “Steve” was promoting and talking about having sex with children and infants. Adult Male A reported that he believed that “Steve” used the Kik account name of yourmister2018 and lived at the SUBJECT PREMISES. Adult Male A provided the Huber Heights Police Department screen prints of iMessages¹ that he recently exchanged with “Steve”.
- 75. In April 2019, the Huber Heights Police Department forwarded me the report documenting the information provided by Adult Male A. I subsequently interviewed Adult Male A on several occasions. In summary, Adult Male A provided the following information:
 - a. Around the fall of 2018, Adult Male A met “Steve” in a group chat on Kik Messenger. “Steve” used the Kik account name of yourmister2018. Adult Male A could not recall the name of this group chat but advised that it was for gay and bi-sexual men (which is consistent with the name of the group chat reported by Kik Interactive Inc., as detailed in paragraph 69).
 - b. After communicating via the group chat, Adult Male A and “Steve” communicated individually with each other on Kik Messenger. “Steve” utilized both the account

¹ iMessages is an instant messaging service developed by Apple Inc. The service allows Apple users to send text messages, documents, photographs, videos, contact information, and group messages over Wi-Fi, a cellular telephone’s data plan, or other forms of Internet access.

names of yourmister2018 and yourmister2019. Adult Male A and “Steve” also communicated with each other via iMessages and telephone calls. “Steve” utilized telephone number 937-304-8099 (hereinafter referred to as “TARGET CELL PHONE-1”) for these communications. They communicated with each other for a period of a few months, ending in or around February 2019. They often talked to each other about sex and other sexually explicit topics.

- c. Adult Male A and “Steve” met each other in person on a few occasions. They met in the garage of the SUBJECT PREMISES on approximately two to three of these occasions. “Steve” said that the SUBJECT PREMISES was his grandmother’s house, and he indicated that he did not live there.
- d. On one occasion when they met in person, Adult Male A and “Steve” tried to guess each other’s names. When Adult Male A guessed the name “Steve”, “Steve” made an expression indicating that this was his name. According to Adult Male A, “Steve” never confirmed that it was his true name.
- e. Sometime after the Christmas holiday, “Steve” said that he wanted to talk to Adult Male A via the Telegram application. Adult Male A created a Telegram account and communicated with “Steve”. Adult Male A could not recall “Steve’s” Telegram account name. During the communications, “Steve” sent Adult Male A one video and approximately three images of what appeared to be child pornography. Adult Male A stated that the images depicted what appeared to be the same female child posing nude. It did not appear to Adult Male A that this child had experienced puberty. Adult Male A stated that the video depicted what appeared to be a female child performing sexual acts on a man. While it appeared to Adult Male A that the female depicted in the video was also a child, Adult Male A could not conclude with complete certainty that she was a child.
- f. “Steve” told Adult Male A that the female depicted in the images and video he sent via Telegram was a foster child with whom he had a sexual relationship. “Steve” did not specify the sexual acts he engaged in with the child or the child’s age. “Steve” also told Adult Male A that he had friends who brought children over to his house, and that he and the friends had sex with these children. “Steve” said that the children were as young as infants.
- g. Shortly after receiving the suspected child pornography files, Adult Male A deleted the files and reported the communications to the Huber Heights Police Department.
- h. Adult Male A provided a physical description of “Steve”. Adult Male A saw “Steve” drive a white Ford Fusion. Adult Male A also saw a Nissan Altima parked in the garage of the SUBJECT PREMISES. “Steve” stated that he worked in Vandalia, Ohio and had an iPhone.
- i. I noted that Adult Male A’s description of “Steve” is mostly consistent with KIRBY’s physical description (although Adult Male A reported a different eye color and height than that of KIRBY).

- ii. Based on records from the Ohio Bureau of Motor Vehicles, I know that there is a white Ford Fusion that is registered to Adult Female A at the SUBJECT PREMISES. Although Adult Male A recalled the Nissan Altima being a different color, the vehicle is consistent with the SUBJECT VEHICLE.
- iii. As noted above in paragraph 65, KIRBY's current sex offender registration paperwork identifies that he works in Vandalia, Ohio.
- i. During one of the interviews, Adult Male A was shown a photographic line-up that depicted six white males, one of which depicted KIRBY. Adult Male A identified that KIRBY was "Steve".

76. At the time that I interviewed Adult Male A in April 2019, he no longer had any of the messages he exchanged with "Steve" on his cellular telephone. However, I reviewed the screen prints that Adult Male A provided to the Huber Heights Police Department. Consistent with the information provided by Adult Male A, I noted that the iMessages included references to "Steve's" alleged comments about having sex with infants. The iMessages also included a comment about the SUBJECT PREMISES. Furthermore, the iMessages included an apparent inquiry by Adult Male A about the alleged child pornography files that "Steve" previously sent. "Steve" indicated in the iMessages that he could show the files to Adult Male A on a computer. Furthermore, "Steve" made comments in the iMessages indicating that he previously had an application on his cellular telephone that hid his files. Below are excerpts of the conversation:

Adult Male A:	You're sketch ab what's on ur phone so you use that app to hide your shit and I'm saying that's ok
Steve:	I have no app anymore. My phone has been scrubbed. Not taking that risk anymore. New year. New me
Adult Male A:	Scrub?
Steve:	Cleaned
Adult Male A:	Of what
Steve:	That app that hide my files
Adult Male A:	Why do you need to hide your files haha
Steve:	You should send me stuff on Kik if you. Or you on here. And because ppl use my phone
Adult Male A:	But you saved those vids of that girl didn't you
Adult Male A:	Are those on a computer we could watch
Steve:	I've created a perv haven't I? Hehe
Adult Male A:	Well??
Adult Male A:	??
Steve:	Yea
Adult Male A:	You still into that
Steve:	Nope

.....

Adult Male A:	You are a weirdo Steven
Steve:	True and so are you
Adult Male A:	You have had sex with infants

Steve: Have I? Oooooor was it a lie
Steve: Just to keep you wanting me
Adult Male A: 5068 Nielson ct. I can get you when ever I want
Steve: You could. Or I moved
Steve: Remember that wasn't my house

Additional FBI Undercover Investigation – Kik Platform, April 2019

77. Based on the information provided by Adult Male A, UCO-1 contacted the user of the yourmister2019 Kik account on or around April 17, 2019. UCO-1 communicated with the yourmister2019 Kik account user on or around April 17, 2019 through April 18, 2019. Below is a summary of these communications via the Kik platform:

- a. In the communications, the yourmister2019 account user indicated that he had teenage children. He further indicated that he did not currently engage in sexual activities with these children, but that he had engaged in sexual activities with other children.
- b. During the exchange of messages, the yourmister2019 account user sent UCO-1 one video file depicting child pornography. The yourmister2019 account user also requested images depicting UCO-1's purported child.
 - i. Based on the context of this conversation and other information noted in the Affidavit, it appeared that the yourmister2019 account user was soliciting child pornography files that depicted UCO-1 and his purported children.
- c. The yourmister2019 account user made a comment indicating that he had a second telephone at another location that contained more child pornography files.
- d. The yourmister2019 account user stated that he had "private" or "homemade" pornography at his home. The yourmister2019 account user described his "private" or "homemade" pornography as being files that depicted him and boys, as well as other fathers and their children.
 - i. Based on my training and experience, I know that offenders often refer to child pornography that they have produced as "private" or "homemade" pornography.
- e. Below is a transcript of UCO-1's chat with the yourmister2019 account user:

UCO-1: Hey
UCO-1: 33 dad here with dau. You ?
yourmister2019: Sons. Age? Active?
UCO-1: Nice
UCO-1: Yes mine is 8
UCO-1: And I have a niece that's 3
UCO-1: Yes active with daughter when she is asleep and active with 3 yo when I see her
UCO-1: What about u how old is yours
yourmister2019: Teens now so I don't get to play but I do have others. Hehe

UCO-1: Nice !!!!
 UCO-1: What ages u have ?
 yourmister2019: Lots of different ones. Do you take requests or have stuff I can see
 UCO-1: I usually do live for live but if u have good yng newer stuff I might
 yourmister2019: I do. I go live randomly since I never know when I'll be with a kid
 UCO-1: Ah ok who u have access and age
 yourmister2019: Ohio here
 UCO-1: I can show I live real quick but can't do much right now cause gf here
 UCO-1: Va here
 yourmister2019: Ok. I'm in bathroom. Go ahead
 UCO-1: What u have in gallery now
 yourmister2019: Not much since this is my public phone lol
 UCO-1: Live stuff from past ? Or stuff from net?
 UCO-1: Ah damn
 UCO-1: Just want to know cool before I send lol
 yourmister2019: *Sends close-up image of what appears to be a male's penis.*
 UCO-1: Cock proves I'm not a cop lol
 UCO-1: I mean I k or you're a dude lol
 UCO-1: I know
 UCO-1: U said u have different stuff but not on u now?
 yourmister2019: Ya.
 UCO-1: Ah ok
 UCO-1: Well I'll be here for a while let me know when u do and we can go from there
 yourmister2019: You can't show live? like you said
 yourmister2019: I found some videos but they aren't of me
 UCO-1: That's fine
 UCO-1: Yes
 yourmister2019: Can I see something so I know your not a cop
 UCO-1: Yes
 UCO-1: *Sends image that depicts what appears to be the chest of a female child wearing clothing (although the image does not depict a real child). A man's hand is touching the child's shirt.*
 yourmister2019: Fuck wow
 UCO-1: Yeah
 yourmister2019: *Sends video file depicting the groin area of what appears to be a white female child who is wearing underwear. What appears to be a black male masturbates his penis. The black male then pulls aside the child's underwear, exposing her nude vagina. He rubs his penis on the child's nude vagina and partially inserts his penis into her vagina. The video is approximately 37 seconds in duration.*
 UCO-1: I'm cool lol
 UCO-1: Mmmmm

UCO-1: *Sends image that depicts what appears to be the chest of a female child wearing clothing (although the image does not depict a real child). A man's hand is pulling aside the child's shirt, exposing her breast.*

yourmister2019: You got anything video of them or what can we do

yourmister2019: How young

yourmister2019: Is she

yourmister2019: Pussy?

UCO-1: She is 8 and yes I can do more

UCO-1: What else u have

yourmister2019: That's a video. Can I get one. I have others like that. Private stuff at home

UCO-1: Oh nice yes I can take a vid once I'm alone . Gf here now so had to sneak those.

UCO-1: Maybe a few more of yours and I'll try to sneak a vid

UCO-1: How old are your homemade stuff at home

yourmister2019: You don't have any saved?

yourmister2019: Of them?

UCO-1: Not the vids , I do live and erase. Been caught once and talked my way out of it so I'm careful

UCO-1: *Sends image that depicts what appears to be the abdomen of a female child wearing underwear and a shirt (although the image does not depict a real child). The child's shirt is pulled up, and part of her breast is exposed.*

UCO-1: ?

yourmister2019: Sorry. Ppl were around

yourmister2019: Hope I didn't lose you

UCO-1: No worries u scared me

UCO-1: Lol

yourmister2019: Nah. You know I'm real. I sent stuff

UCO-1: Yes . I sent u live so u know I'm legit lol

yourmister2019: Yes and hot

yourmister2019: Love to train her with you

UCO-1: Like i said I can get live vids once alone

UCO-1: Always wanted to see her with someone else be so hot

yourmister2019: Bet she sucks great coxk and will love it in her cunt and ass

UCO-1: Yes !

yourmister2019: You done that

UCO-1: Nor ads

UCO-1: Tip in pussy

UCO-1: Ass

yourmister2019: While awake

UCO-1: Mostly while she is asleep now

UCO-1: What others u have with u

yourmister2019: Couple younger

UCO-1: And what homemade stuff u have

UCO-1: Mmmmmm

yourmister2019: Mainly me with boys. Friends brothers. Couple other dads

and theirs
UCO-1: Younger the better miss to baby/toddler days
UCO-1: Mmmm
UCO-1: Nice
yourmister2019: Oh
yourmister2019: You still near her
UCO-1: Can be
UCO-1: What else u have
yourmister2019: Videos of kids with men
UCO-1: Mmm
yourmister2019: Ya but how soon you wanna send some stuff. I need to get
back. I'm in bathroom
UCO-1: Can u sent what u have to I did send live :)
yourmister2019: I sent a video though. I only have three or four on here.
Trying to stretch them
UCO-1: Hmm
yourmister2019: Ok

Service of Administrative Subpoenas

78. On or around May 10, 2019, an FBI investigator served a subpoena to Kik Interactive Inc. requesting subscriber information for the Kik account names of mymister2018, yourmister2018, and yourmister2019, as well as logs of IP addresses utilized to access these accounts and transmit messages. Kik Interactive Inc. also provided additional records for the mymister2018 account as part of its report to the Royal Canadian Mounted Police (as detailed in paragraphs 68 to 71).
79. Records provided by Kik Interactive Inc. in response to the subpoena and as part of its report to the Royal Canadian Mounted Police included the following information for the mymister2018 Kik account:
- a. Kik Interactive Inc.'s records identified that a Kik account with an account name of mymister2018 and a profile name of "My Mister" was created on or around May 31, 2018. The email address mymister2018@yahoo.com was associated with the account profile.
 - b. Kik Interactive Inc. provided a log of IP addresses utilized to access the mymister2018 account during the approximate time period of May 31, 2018 through June 8, 2018. These records identified that the following IP addresses were utilized to access the account and transmit messages:
 - i. IP addresses associated with Verizon's cellular telephone network were utilized to access the account and transmit messages on approximately 139 occasions. The use of IP addresses associated with Verizon's network is consistent with someone using the data plan from his/her cellular telephone to access the Internet – and is also consistent with the use of TARGET CELL PHONE-2 (which is serviced by Verizon).

- ii. Four other IP addresses serviced by Charter Communications were also utilized to access the account and transmit messages: 71.79.52.128 (utilized on approximately 133 occasions), 75.186.19.61 (utilized on approximately 49 occasions), 74.142.189.50 (utilized on approximately five occasions), and 24.166.11.92 (utilized on approximately three occasions).
 - c. Kik Interactive Inc.'s records identified that an iPhone was used to access the mymister2018 account on or around June 5, 2018.
- 80. Records provided by Kik Interactive Inc. in response to the subpoena included the following information for the yourmister2018 Kik account:
 - a. Kik Interactive Inc.'s records identified that a Kik account with an account name of yourmister2018 and a profile name of "Your Mister" was created on or around November 9, 2018. The email address yourmister2018@yahoo.com was associated with the account profile.
 - b. Kik Interactive Inc. provided a log of IP addresses utilized to access the yourmister2018 account during the approximate time period of April 13, 2019 through May 10, 2019. These records identified that the following IP addresses were utilized to access the account and transmit messages:
 - i. IP addresses associated with Verizon's cellular telephone network were utilized to access the account and transmit messages on approximately 19 occasions. IP addresses associated with Sprint's network were utilized to access the account and transmit messages on approximately 163 occasions. The use of IP addresses associated with Verizon's and Sprint's networks is consistent with someone using the data plan from his/her cellular telephone to access the Internet – and is also consistent with the use of TARGET CELL PHONE-1 (which is serviced by Sprint Corporation) and TARGET CELL PHONE-2 (which is serviced by Verizon).
 - ii. An IP address serviced by Leaseweb USA was utilized to access the account and transmit messages on approximately eight occasions.
 - 1. Based on Internet research, I have determined that Leaseweb USA is a global Internet services company based in the Netherlands. The company offers customers a variety of network solutions, to include virtual servers and private networks.
 - iii. Two IP addresses serviced by Charter Communications were utilized to access the account and transmit messages: 74.140.165.102 (which was utilized on approximately 428 occasions) and 174.97.108.225 (which was utilized on approximately 12 occasions).
 - c. Kik Interactive Inc.'s records identified that an iPhone was used to access the yourmister2018 account on or around February 14, 2019.

81. Records provided by Kik Interactive Inc. in response to the subpoena included the following information for the yourmister2019 Kik account:
- a. Kik Interactive Inc.'s records identified that a Kik account with an account name of yourmister2019 and a profile name of "Your Mister" was created on or around January 4, 2019. The email address yourmister2019@yahoo.com was associated with the account profile.
 - b. Kik Interactive Inc. provided a log of IP addresses utilized to access the yourmister2019 account during the approximate time period of April 13, 2019 through May 10, 2019. These records identified that the following IP addresses were utilized to access the account and transmit messages:
 - i. IP addresses associated with Verizon's cellular telephone network were utilized to access the account and transmit messages on approximately 435 occasions. The use of IP addresses associated with Verizon's network is consistent with someone using the data plan from his/her cellular telephone to access the Internet – and is also consistent with the use of TARGET CELL PHONE-2 (which is serviced by Verizon).
 - ii. IP addresses serviced by Leaseweb USA were utilized to access the account and transmit messages on approximately 795 occasions.
 - iii. Two IP addresses serviced by Charter Communications were utilized to access the account and transmit messages: 74.140.165.102 (which was utilized on approximately 193 occasions) and 174.97.108.225 (which was utilized on approximately 20 occasions).
 - iv. Two IP addresses serviced by AT&T were utilized to access the account and transmit messages: 104.62.2.87 (which was utilized on approximately 14 occasions) and 76.192.65.81 (which was utilized on approximately 28 occasions).
 - v. An IP address serviced by the Ohio Public Libraries Information Network was utilized to access the account and transmit messages on approximately one occasion.
 - c. Kik Interactive Inc.'s records identified that an iPhone was used to access the yourmister2019 account on or around May 1, 2019.
82. As part of the investigation, approximately three administrative subpoenas were served to Charter Communications requesting subscriber information for the six IP addresses utilized to access the mymister2018, yourmister2018, and yourmister2019 Kik accounts on a sample of dates and times that they were utilized to transmit messages. Records received from Charter Communications in response to the subpoenas provided the following information:
- a. The IP address of 71.79.52.128 (which was utilized to transmit approximately 133 messages for the mymister2018 Kik account) was subscribed to Adult Female A at the

SUBJECT PREMISES.

- b. The IP address of 74.140.165.102 (which was utilized to transmit approximately 428 messages for the yourmister2018 Kik account and approximately 193 messages for the yourmister2019 Kik account) was subscribed to Adult Female A at the SUBJECT PREMISES.
 - c. The IP address of 174.97.108.225 (which was utilized to transmit approximately 12 messages for the yourmister2018 Kik account and approximately 20 messages for the yourmister2019 account) was subscribed to KIRBY at 3150 Charlotte Mill Road in Dayton, Ohio.
 - i. The 3150 Charlotte Mill Road address is not listed on KIRBY's driver's license or sex offender registration paperwork.
 - ii. I know that KIRBY resided at 3150 Charlotte Mill Road, Dayton, Ohio, prior to his arrest in 2012. Based on records from the Montgomery County (Ohio) Auditor, KIRBY currently owns this residence. The investigation has identified that Adult Female B, along with her and KIRBY's children, currently reside at this residence.
 - d. The IP address of 74.142.189.50 (which was utilized to transmit approximately five messages for the mymister2018 Kik account) was subscribed to the Guest Inn-Suites at 800 West 8th Street, Cincinnati, Ohio.
 - e. Charter Communications no longer had records associated with the subscriber of the IP addresses 75.186.19.61 (which was utilized to transmit approximately 49 messages for the mymister2018 Kik account) and 24.166.11.92 (which was utilized to transmit approximately three messages for the mymister2018 Kik account), as the requested dates were past Charter Communications' retention period.
83. Also as part of the investigation, an administrative subpoena was served to AT&T requesting subscriber information for the two IP addresses utilized to access the yourmister2019 Kik account on a sample of dates and times that they were utilized to transmit messages. Records received from AT&T in response to the subpoena provided the following information:
- a. The IP address of 104.62.2.87 (which was utilized to transmit approximately 14 messages for the yourmister2019 Kik account) was subscribed to an adult male who will be referred to for purposes of this Affidavit as "Adult Male B" at an address in Dayton, Ohio.
 - b. The IP address of 76.192.65.81 (which was utilized to transmit approximately 28 messages for the yourmister2019 Kik account) was subscribed to Fitness International LLC. The service address for the account was LA Fitness' location in Beavercreek Ohio.
84. An administrative subpoena was served to Leaseweb USA requesting subscriber information for a sample of four of the IP addresses utilized to access the yourmister2018 and

yourmister2019 accounts. Records provided by Leaseweb USA in response to the subpoena identified that each of the IP addresses were assigned to ProtonVPN in Switzerland.

- a. Based on Internet research, I know that ProtonVPN provides VPN's to customers around the world. The company's website notes that ProtonVPN offers secure VPN's that send Internet traffic through an encrypted VPN tunnel. The company's website also notes that as a Swiss VPN provider, the company does not log users' activities or share data with third parties.
85. On or around April 22, 2019, an administrative subpoena was served to the Quality Inn and Suites (which appears to be the new name for the Guest Inn-Suites) located at 800 West 8th Street in Cincinnati, Ohio, requesting information for any hotel stays by KIRBY. Records received in response to the subpoena indicated that KIRBY stayed at the hotel from the evening of June 6, 2018 through the morning of June 7, 2018. This time period covered the approximately five occasions in which the IP address subscribed to the Guest-Inn Suites was utilized to transmit messages for the mymister2018 Kik account (as detailed above in paragraph 79(b)(ii)).
 86. On or around September 10, 2018, an administrative subpoena was served to Verizon requesting subscriber information for TARGET CELL PHONE-2 (the telephone number that KIRBY reported having to PO Owens). Records received in response to the subpoena identified that the telephone number is subscribed to STEPHEN KIRBY at an address in London, Ohio. Based on this London, Ohio address, it appears that KIRBY's father (STEPHEN KIRBY I) is the subscriber. It should be noted that PO Owens previously learned that KIRBY's father had set up KIRBY's telephone account. Verizon's records indicated that the telephone number was activated on or around May 15, 2018 (shortly after KIRBY was released from the custody of the Bureau of Prisons).
 87. On or around April 18, 2019, an administrative subpoena was served to Sprint Corporation requesting subscriber information and incoming/outgoing call and text message details for TARGET CELL PHONE-1 (the telephone number Adult Male A used to communicate with "Steve"), as well as the make and model of the device that utilized this telephone number. Records received in response to the subpoena provided the following information:
 - a. The telephone number was subscribed to "STEVE KIRBY" at 3150 Charlotte Mill Road, Dayton, Ohio (the address where Adult Female B and her and KIRBY's children reside). The account was activated on or around November 8, 2018 (approximately seven months after KIRBY was released from the custody of the Bureau of Prisons), and it was active as of the date of the subpoena (on or around April 18, 2019).
 - b. Consistent with the information provided by Adult Male A, the incoming/outgoing call and text message details identified that approximately five voice calls and approximately two text messages were exchanged between TARGET CELL PHONE-1 and Adult Male A's telephone number during the approximate time period of February 16, 2019 through February 21, 2019.
 - i. It should be noted that because iMessages utilize Internet service to transmit messages, the iMessages do not appear on the incoming/outgoing text message

details of the telephone provider. As such, the iMessages exchanged between Adult Male A and KIRBY are not reflected in the telephone records for TARGET CELL PHONE-1.

- c. Consistent with the information provided by Adult Male A, Sprint Corporation's records identified that the device utilizing TARGET CELL PHONE-1's telephone number was an iPhone SE, gray in color. Sprint Corporation's records further identified that the device had an Electronic Serial Number of 089587943210027077 and International Mobile Subscriber Identity (IMSI) of 310120242722519.

Review of Kik and Telegram Profiles

88. On or around April 14, 2019 and May 9, 2019, I conducted an Internet search for publicly available Kik profiles. I located profiles for the mymister2018, yourmister2018, and yourmister2019 Kik accounts. The Kik account for the mymister2018 account did not contain a profile picture, and it was not clear if the account was still active. I noted that the yourmister2018 and yourmister2019 Kik accounts utilized a profile name of "Your Mister" and the same profile picture – a picture of what appeared to be a person's wrist with the word "Always" tattooed on it. Both accounts (yourmister2018 and yourmister2019) appeared to presently be open and/or active. The use of the same profile picture, the same profile name, and nearly the same account name is consistent with the same person utilizing the yourmister2018 and yourmister2019 accounts (as reported by Adult Male A).
89. On or around May 9, 2019, an FBI investigator accessed publicly available information on Telegram Messenger. Consistent with information provided by Adult Male A, a Telegram account was located that was associated with TARGET CELL PHONE-1. This Telegram account had a user name of "yourmister2018" and a profile name of "Daddy Mister". The profile information indicated that the account was online as recently as May 9, 2019.

Location Information for TARGET CELL PHONE-1 and TARGET CELL PHONE-2

90. On or around April 26, 2019, two search warrants were authorized by the United States District Court for the Southern District of Ohio authorizing (1) the release of historical subscriber information, incoming/outgoing call and text message transactional records, Internet connectivity data, and cell site information by Sprint Corporation for TARGET CELL PHONE-1 for the approximate time period of November 8, 2018 through April 26, 2019 and (2) the release of prospective location information (i.e., cell site, cell sector, and GPS information, commonly referred to as a "Ping Order") by Sprint Corporation for TARGET CELL PHONE-1 for a period of 30 days. On or around April 29, 2019, two additional search warrants were authorized by the United States District Court for the Southern District of Ohio authorizing (1) the release of historical subscriber information, incoming/outgoing call and text message transactional records, Internet connectivity data, and cell site information by Verizon for TARGET CELL PHONE-2 for the approximate time period of April 23, 2018 through April 29, 2019 and (2) the release of prospective location information (i.e., cell site, cell sector, and GPS information, commonly referred to as a "Ping Order") by Verizon for TARGET CELL PHONE-2 for a period of 30 days.
91. An FBI agent who has training and experience in examining cellular telephone data has

conducted an initial review of historical records provided by Sprint Corporation for TARGET CELL PHONE-1 (the telephone number Adult Male A used to communicate with “Steve” and that is associated with the Telegram account). In summary, the records provided the following information:

- a. Sprint Corporation’s records identified that only approximately 80 telephone calls and approximately 123 text messages were sent or received by TARGET CELL PHONE-1 during the approximate time period of November 8, 2018 through April 26, 2019. Only approximately 18 of the 80 telephone calls contained call durations that were more than 60 seconds.
 - i. Based on this information, it does not appear that TARGET CELL PHONE-1 was frequently utilized to make and receive telephone calls and text messages.
 - ii. Given the minimal call activity, there was not a lot of cell tower data to be used for analysis.
- b. Although there was a fairly insignificant number of telephone calls and text messages, Sprint Corporation’s records identified that TARGET CELL PHONE-1 accessed Internet data on thousands of occasions during the approximate time period of January 1, 2019 through April 26, 2019.
- c. During the approximate time period of January 1, 2019 through April 26, 2019, TARGET CELL PHONE-1 made or received telephone calls utilizing the closest cell tower to the SUBJECT PREMISES on approximately 11 occasions.
 - i. This information is consistent with TARGET CELL PHONE-1 being at the SUBJECT PREMISES on these approximately 11 occasions. However, given the geographic area that the cell tower covers, the precise location of the device could not be determined.
 - ii. It should be noted that there were other occasions in which other cell towers near the SUBJECT PREMISES were utilized by TARGET CELL PHONE-1 to make or receive telephone calls. Because cellular telephones do not always utilize the closest cell towers, it is possible that TARGET CELL PHONE-1 was at or near the SUBJECT PREMISES on these other occasions as well.
- d. Also during the approximate time period of January 1, 2019 through April 26, 2019, there were numerous occasions in which TARGET CELL PHONE-1 accessed Internet data utilizing cell towers that cover the geographic area of Huber Heights, Ohio (consistent with the location of the SUBJECT PREMISES). For example, during the approximate time period of April 20, 2019 through April 26, 2019, TARGET CELL PHONE-1 accessed Internet data on more than 600 occasions utilizing cell towers that cover the geographic area of Huber Heights, Ohio – many of which were during the overnight hours.
- e. TARGET CELL PHONE-1 did not access Internet data or make any telephone calls during the morning hours of April 18, 2019 (the time period when the yourmister2019

Kik account user communicated with and sent child pornography to UCO-1, as detailed above in paragraphs 77(a) through 77(e)).

- i. This information, as well as other information detailed in the Affidavit, is indicative that TARGET CELL PHONE-2 was utilized to communicate with UCO-1 on this date.

92. The prospective location information ("Ping Order") for TARGET CELL PHONE-1 was monitored during the approximate time period of April 29, 2019 through May 8, 2019. It should be noted that the location information provided by Sprint Corporation included degrees of uncertainty of up to approximately four and a half miles. As such, the precise locations of TARGET CELL PHONE-1 could not be determined. It was noted that there were times throughout the day that TARGET CELL PHONE-1 appeared to be powered off, and as such, no location information was available during those time periods. Below is a summary of location information for TARGET CELL PHONE-1 during the times that it was turned on and location information was available:
- a. TARGET CELL PHONE-1 was primarily in the geographic area of the SUBJECT PREMISES during the overnight hours.
 - b. TARGET CELL PHONE-1 was consistently in the geographic area of KIRBY's place of employment in Vandalia, Ohio during the morning and early afternoon hours on week days.
 - c. During the late afternoon hours of May 1, 2019, TARGET CELL PHONE-1 was powered off. It was turned on throughout the morning and early afternoon hours, and after it was turned off, it was turned back on during much of the evening hours.
 - i. It was noted that the time period that the device was powered off coincided with when PO Owens was conducting a home visit at the SUBJECT PREMISES. PO Owens informed me that he notified KIRBY in advance of the date and time of the home visit.
 - ii. Based on this and other information noted in the Affidavit, it appears that KIRBY powered off TARGET CELL PHONE-1 in an attempt to conceal it from PO Owens.
 - d. TARGET CELL PHONE-1 was consistently in the same geographic location as TARGET CELL PHONE-2 during times that both devices were powered on and location information was available. This information is consistent with the same person utilizing both devices.
 - e. TARGET CELL PHONE-1 did not travel outside of the Southern District of Ohio.
93. An FBI agent who has training and experience in examining cellular telephone data has conducted an initial review of the historical records provided by Verizon for TARGET CELL PHONE-2 (the telephone KIRBY reported having to PO Owens). In summary, the records provided the following information:

- a. The device utilizing TARGET CELL PHONE-2 was an Apple iPhone 7 Plus bearing IMEI number 355376083197462.
- b. Verizon's records identified that TARGET CELL PHONE-2 was regularly used to make and receive telephone calls and text messages during the approximate time period of May 15, 2018 through April 29, 2019. Verizon's records also identified that TARGET CELL PHONE-2 accessed Internet data on thousands of occasions during the approximate time period of May 15, 2018 through April 29, 2019.
- c. During the approximate time period of January 1, 2019 through April 26, 2019, TARGET CELL PHONE-2 made or received telephone calls utilizing the closest cell tower to the SUBJECT PREMISES on more than 100 occasions.
 - i. This information is consistent with TARGET CELL PHONE-2 being at the SUBJECT PREMISES on these more than 100 occasions. However, given the geographic area that the cell tower covers, the precise location of the device could not be determined.
 - ii. It should be noted that there were other occasions in which other cell towers near the SUBJECT PREMISES were utilized by TARGET CELL PHONE-2 to make or receive telephone calls. Because cellular telephones do not always utilize the closest cell towers, it is possible that TARGET CELL PHONE-2 was at or near the SUBJECT PREMISES on these other occasions as well.
- d. On or around April 18, 2018, TARGET CELL PHONE-2 made a telephone call at approximately 11:35 a.m. (which is in close proximity to when the yourmister2019 Kik account user communicated with and sent child pornography to UCO-1, as detailed above in paragraphs 77(a) through 77(e)). This telephone call utilized one of the cell towers that covers the geographic location of KIRBY's place of employment in Vandalia, Ohio. Later in the day, at approximately 6:16 p.m., TARGET CELL PHONE-2 made a telephone call using a cell tower that covers the geographic area of 3150 Charlotte Mill Road in Moraine, Ohio (the location where Adult Female B and her and KIRBY's children reside, as detailed above in paragraph 82(c)(ii)). During the late evening hours of April 18, 2019 and early morning hours of April 19, 2019, TARGET CELL PHONE-2 made telephone calls utilizing cell towers that cover the geographic area of the SUBJECT PREMISES.
 - i. This cell tower data is consistent with KIRBY being at work when he communicated with UCO-1 and returning to the SUBJECT PREMISES later that night.
 - ii. As detailed above (in paragraphs 77(a) through 77(e)), the yourmister2019 Kik account user indicated in his communications with UCO-1 on April 18, 2019 that he was using his "public" phone, that he had another phone that had more child pornography files, and that he had access to more child pornography files (including "homemade" or "private" files) at his residence.

- e. The cell tower data for TARGET CELL PHONE-2 was compared to the cell tower data for TARGET CELL PHONE-1 during the approximate time period of March 15, 2019 through April 26, 2019. Due to the minimal call activity for TARGET CELL PHONE-1 (as detailed above in paragraph 91(a)), there were not many occasions when both devices were utilized during the same time periods. However, approximately four occasions were noted when TARGET CELL PHONE-1 and TARGET CELL PHONE-2 were utilized within relative close proximity to each other (i.e., less than two hours of each other). On these approximately four occasions, both telephones utilized cell towers that cover the same general geographic areas. These four occasions included one instance in which both telephones were utilized in the geographic area of the SUBJECT PREMISES and approximately three instances in which both devices were utilized in the geographic area of Beavercreek, Ohio. This information is consistent with the two devices being located at the same locations.
94. The prospective location information ("Ping Order") for TARGET CELL PHONE-2 was monitored during the approximate time period of April 29, 2019 through May 8, 2019 (with the exception of the approximate time period of the afternoon hours of April 30, 2019 through the afternoon hours of May 1, 2019, during which time data was not collected due to an administrative error). It should be noted that the location information provided by Verizon included degrees of uncertainty of up to approximately three and six-tenths miles. As such, the precise locations of TARGET CELL PHONE-2 could not be determined. Below is a summary of the prospective location information for TARGET CELL PHONE-2:
- a. TARGET CELL PHONE-2 was primarily in the geographic area of the SUBJECT PREMISES during the overnight hours.
 - b. TARGET CELL PHONE-2 was consistently in the geographic area of KIRBY's place of employment in Vandalia, Ohio during the morning and early afternoon hours on week days.
 - c. TARGET CELL PHONE-1 was consistently in the same geographic location as TARGET CELL PHONE-2 during times that both devices were powered on and location information was available. This information is consistent with the same person utilizing both devices.
 - d. TARGET CELL PHONE-2 did not travel outside of the Southern District of Ohio.

Surveillance Activities

- 95. On or around May 2, 2019, an FBI agent observed the SUBJECT VEHICLE parked in the parking lot of KIRBY's place of employment in Vandalia, Ohio. Location information for both TARGET CELL PHONE-1 and TARGET CELL PHONE-2 indicated that both devices were in this geographic location around the approximate time of the surveillance activity.
- 96. On the morning of on or around May 3, 2019, I observed the SUBJECT VEHICLE drive away from the SUBJECT PREMISES and travel in a direction consistent with traveling to KIRBY's place of employment in Vandalia, Ohio. Approximately one-half hour later, I observed the SUBJECT VEHICLE parked in the parking lot of KIRBY's place of employment. Location

information for both TARGET CELL PHONE-1 and TARGET CELL PHONE-2 indicated that both devices were in the geographic locations of the SUBJECT PREMISES and then at the place of employment around the approximate times of the surveillance activities.

97. During the late afternoon hours of on or around May 6, 2019, another FBI agent and I observed the SUBJECT VEHICLE parked in the parking lot of a LA Fitness in Beavercreek, Ohio. The other FBI agent also observed KIRBY inside this fitness center. Location information for TARGET CELL PHONE-2 indicated that it was also in this geographic location around the approximate time of the surveillance activity. TARGET CELL PHONE-1 was powered off at the time of the surveillance activity, but it was powered on approximately one hour later. The location information for TARGET CELL PHONE-1 at the time that it was powered on indicated that it was also in the geographic location of LA Fitness.
- a. As detailed above, an IP address receiving service at LA Fitness' location in Beavercreek, Ohio was utilized to transmit messages for the yourmister2019 Kik account. It was noted that one of the dates that this IP address was utilized to transmit messages for the yourmister2019 Kik account was on May 6, 2019, during the same approximate time period of the surveillance activity.
98. On the morning of on or around May 9, 2019, another FBI agent observed a white male who resembled KIRBY exit the front door of the SUBJECT PREMISES and enter the detached garage. The agent then observed the SUBJECT VEHICLE exit the garage and drive away from the SUBJECT PREMISES. The FBI agent and I surveilled the SUBJECT VEHICLE as it traveled to KIRBY's place of employment in Vandalia, Ohio. Location information for TARGET CELL PHONE-2 indicated that the device was in the geographic locations of the SUBJECT PREMISES and then the place of employment around the approximate times of the surveillance activities. TARGET CELL PHONE-2 was powered off at the time of the surveillance activity.

Execution of Search Warrants

99. On or around May 9, 2019, search warrants were authorized by the United States District Court for the Southern District of Ohio for the SUBJECT PREMISES, SUBJECT VEHICLE, KIRBY's person, TARGET CELL PHONE-1, and TARGET CELL PHONE-2. Agents and task force officers of the FBI executed these search warrants on or around May 10, 2019. KIRBY was the only individual present when agents and officers arrived at the SUBJECT PREMISES to execute the warrants. Among other items, the following items were seized pursuant to the search warrants:
- a. An iPhone 7 Plus (consistent with TARGET CELL PHONE-2) and an iPhone SE (consistent with TARGET CELL PHONE-1) were seized from KIRBY's pants pocket.
- b. An Apple watch bearing serial number FH7QM44MG9J6 was seized from KIRBY's wrist.
- c. An Alcatel cellular telephone was seized from the center console of the SUBJECT VEHICLE.

- d. A Dell All-in-One computer was seized from the family room of the residence. A note was taped to the base of the computer that stated "SMX", "[csikirby@gmail](mailto:csikirby@gmail.com)" (an apparent reference to csikirby@gmail.com), and what appeared to be a password.
 - i. PO Owens advised that he has not authorized KIRBY to use the Dell All-in-One computer, and that KIRBY has denied using it.
 - e. A micro SD card was seized from a locked safe under a bed in what was identified as KIRBY's bedroom.
 - f. An online transaction record for an iPhone SE (consistent with TARGET CELL PHONE-1) was seized from the trunk of the SUBJECT VEHICLE. This record was dated November 8, 2018 (consistent with the activation date of TARGET CELL PHONE-1, as detailed in Sprint Corporation's records described in paragraph 87(a)). The transaction record appeared to be printed by the Best Buy store in Fairborn, Ohio. The customer name on the record was "STEVE KIRBY"; and the customer address on the record was 3150 Charlotte Mill Road in Dayton (again consistent with the subscriber information for TARGET CELL PHONE-1, as detailed in Sprint Corporation's records described in paragraph 87(a)). The customer's telephone number was listed as 937-684-5792 (the telephone number of TARGET CELL PHONE-2), and the customer's email address was listed as riversidepresident2006@yahoo.com.
 - i. It should be noted that KIRBY has not informed PO Owens about the use of the email address riversidepresident2006@yahoo.com. As such, he is forbidden by the terms of his probation from utilizing this email account.
 - ii. It should also be noted that during the previous investigation conducted from 2011 through 2013, the examination of KIRBY's electronic devices indicated that he utilized the riversidepresident2006@yahoo.com account.
100. During the execution of the search warrants, KIRBY agreed to be interviewed after being advised of his Miranda rights. Below is a summary of some of the information provided by KIRBY during the interview:
- a. Since his release from the Bureau of Prisons' custody, KIRBY has resided at the SUBJECT PREMISES with Adult Female A. No one else resided with KIRBY and Adult Female A at this residence. Adult Female A had been in Florida since approximately December 2018, and KIRBY had lived at the residence alone since that time.
 - b. The larger iPhone that was seized from his pants pocket (the iPhone 7 Plus, consistent with TARGET CELL PHONE-2) belonged to KIRBY. The telephone number for this device was 937-684-5792 (the telephone number of TARGET CELL PHONE-2).
 - c. KIRBY claimed that the smaller iPhone seized from his pants pocket (the iPhone SE, consistent with TARGET CELL PHONE-1) belonged to a friend. KIRBY would not provide the name of this friend. KIRBY also claimed that he only had the iPhone SE

for approximately one month. KIRBY stated that he did not know who the telephone account is subscribed to, who the telephone provider was, or who paid the bills for the iPhone.

- i. As detailed above in paragraph 99(f), a transaction record for what appears to be this same iPhone SE was located in the trunk of the SUBJECT VEHICLE. Also as detailed above in paragraph 87(a), records from Sprint Corporation identified that TARGET CELL PHONE-1 (which utilizes an iPhone SE) is subscribed to in KIRBY's name.
 - d. KIRBY stated that he utilized his thumbprint to unlock both the iPhone SE and the iPhone 7 Plus. KIRBY refused to provide the numerical passcodes for these devices.
 - e. At some points in the interview, KIRBY stated that his friends, relatives, and/or children used his iPhones and knew the passcodes to the devices. However, at another point in the interview, KIRBY recanted these statements. At yet another point in the interview, KIRBY stated that he did not want to answer questions about whether or not anyone else had used his iPhones. KIRBY would not provide the names of any friends who supposedly used his iPhones.
 - f. KIRBY denied viewing child pornography since his release from prison.
 - g. KIRBY initially denied using the Kik Messenger and Telegram applications since his release from prison. When asked again later in the interview about the possible use of Kik Messenger since his release from prison, KIRBY responded that he did not want to answer the question.
 - h. KIRBY denied engaging in sexual activities with any children. KIRBY acknowledged that prior to his period of incarceration, he had told others with whom he chatted that he had engaged in sexual activities with children. KIRBY stated that these prior statements were untrue and only represented his fantasies.
 - i. KIRBY denied that he had ever backed up his iPhones or that he utilized cloud storage services such as Dropbox or Mega.
 - j. KIRBY denied utilizing any email addresses other than the one he was authorized to utilize for job searches – that being sekirby2@gmail.com.
 - k. KIRBY stated that the Dell All-in-One computer belonged to Adult Female A. KIRBY stated that there were a few occasions when he had helped Adult Female A fix computer problems, but he only fixed the computer while she was present. KIRBY otherwise denied using the Dell All-in-One computer. He also denied knowing the password to log onto the computer.
101. A preliminary examination has been conducted of the Dell All-in-One computer. Below is a summary of some of the information obtained during the examination conducted to-date:
- a. At least approximately nine images of child pornography were recovered from the

deleted space of the computer. Because the files were recovered from the deleted space, their file names and metadata (such as file create dates) were not recovered. By way of example, two of the images are described as follows:

- i. Image 1: The image depicts what appears to be a nude infant male child lying on his stomach. What appears to be a penis is inserted into the child's anus.
 - ii. Image 2: The image depicts what appears to be a nude pre-pubescent white male child lying on his back. An object is inserted into the child's anus.
- b. At least approximately seven images and fifteen videos were recovered from the computer that depicted what appears to be teenage or young adult males engaged in sexually explicit conduct. Although I was not able to identify the ages of these males with certainty, it is possible that at least some of them may be juveniles and that some of the files may depict additional child pornography. Furthermore, review of the metadata for the fifteen videos indicated that they were saved onto the computer during the approximate time period of January 30, 2019 through May 6, 2019 (the time period that Adult Female A was in Florida and that KIRBY was living at the house by himself, as detailed above in paragraph 100(a)).
- c. At least approximately eleven images of child erotica were recovered from the deleted space of the computer. By way of example, one of the images depicts what appears to be a male holding his penis next to the face of what appears to be an infant child.
- d. Search terms utilized to conduct searches on various Internet browsers were recovered from the computer. Based on my training and experience, some of the search terms appear to be consistent with someone searching for child pornography and child abuse material. By way of example, the following search terms were recovered from the Internet browsers: "sammy child porn series", "sammy cp series", "boy cp series", and "zach carolina rape daughter".
- e. Approximately forty-one documents were saved on the computer that contained KIRBY's name.
- f. Partial fragments of various email messages were recovered from the computer. These messages related to the following email accounts: csikirby@gmail.com, csikirby82@gmail.com, and riversidepresident2006@yahoo.com. Two of the partial email fragments were messages that were sent to riversidepresident2006@yahoo.com by an email address associated with the Google website, both dated on or around June 5, 2018. These messages stated that the riversidepresident2006@yahoo.com email address was listed as the recovery² email address for the Google accounts csikirby82@gmail.com and csikirby@gmail.com, and that both of the Google accounts had been signed into from a new Apple device.

² Based on my training and experience, I know that many email and other Electronic Service Providers often request users to identify a backup or recovery email address for the users' accounts. The Electronic Service Providers will send messages to the backup account in the event that a user is locked out of his/her account, if the Electronic Service Provider needs to perform an enhanced verification of the user's identity, and/or if the Electronic Service Provider identifies suspicious or new activity on a user's account.

- i. PO Owens has not authorized KIRBY to utilize the **csikirby@gmail.com**, **csikirby82@gmail.com**, and **riversidepresident2006@yahoo.com** email addresses. As such, KIRBY is forbidden by the terms of his probation from utilizing these accounts.
- ii. KIRBY was born in 1982. Based on my training and experience, I know that individuals sometimes add their birth year to the end of their email addresses.
- g. The Chrome Internet browser had the following information saved in the Chrome autofill profiles³:
 - i. 937-684-5792 (TARGET CELL PHONE-2),
 - ii. Stephen Kirby,
 - iii. Stephen Kirby II,
 - iv. **riversidepresident2006@yahoo.com**,
 - v. yourmister2019, and
 - vi. 5068 Nielson Court, Dayton, Ohio (the SUBJECT PREMISES).
- h. The Chrome browser also had the following login email addresses saved in the browser history: **csikirby82@gmail.com**, **sekirby2@gmail.com** (the email address that PO Owens authorized KIRBY to utilize), and **riversidepresident2006@yahoo.com**.
- i. The Internet history for computer identified that the Omegle website had been accessed on a number of occasions, as recently as on or around May 7, 2019 (the time period that Adult Female A was in Florida and that KIRBY was living at the house by himself, as detailed above in paragraph 100(a)).
- j. The Internet history for the computer identified that the OneDrive, Dropbox, and Google Drive cloud storage websites had been accessed on a number of occasions. The OneDrive website (including the URL to log into OneDrive accounts) had been accessed as recently as on or around April 1, 2019 (the time period of which KIRBY identified that Adult Female A was in Florida and that he was living at the house by himself, as detailed above in paragraph 100(a)). The Google Drive website had been accessed as recently as on or around April 26, 2019 (again the time period that Adult Female A was in Florida and that KIRBY was living at the house by himself, as detailed above in paragraph 100(a)). The dates that the Dropbox website were accessed were not recovered.

³ When users log into their Google account within Chrome on any platform, Google syncs the users' history, bookmarks, settings, and almost all information saved within the previous browser sessions. Chrome has a built-in autofill feature that allows users to automatically fill out forms on an Internet page. Chrome does this by auto saving users' form history and including it with the data that is synced between browsers. Autofill data is saved on the computer's local disk drive and can be recovered during computer examinations.

- k. The OneDrive program application was installed on the computer, and it was last updated on or around May 8, 2019. Data was recovered for one of the logins to the OneDrive application. This data indicated that the email address of csikirby@gmail.com was utilized to log into a OneDrive account.
102. The two iPhones and the Alcatel cellular telephone seized pursuant to the search warrant have not been examined as of this time due to their locked states. A preliminary examination has been conducted of the micro SD card located in the locked safe in KIRBY's bedroom. Below is a summary of some of the information obtained during the examination conducted to-date:
- a. More than eighty images of child pornography were recovered from the deleted space of the SD card. Because the files were recovered from the deleted space, their file names and metadata (such as file create dates) were not recovered. By way of example, two of the images are described as follows:
 - i. Image 1: The image depicts what appears to be a nude toddler-aged male child lying on his back. His diaper is open, and his shirt is pulled up around his upper chest. What appears to be a penis is inserted into the child's anus.
 - ii. Image 2: The image depicts what appears to be a pre-pubescent female child lying on her back. She is not wearing pants, and her shirt is pulled up around her chest. What appears to be a penis is inserted into the child's vagina.
 - b. A number of other images were recovered from the deleted space of the SD card that depicted what appears to be teenage or young adult males engaged in sexually explicit conduct. Although I was not able to identify the ages of these males with certainty, it is possible that at least some of them may be juveniles and that some of the files may depict additional child pornography.
 - c. More than two hundred images of anime child pornography were recovered from the deleted space of the SD card.
 - d. More than ninety images of KIRBY were recovered from the deleted space of the SD card, including images that depict KIRBY engaged in sexually explicit conduct.
 - e. A document entitled "Password" was saved on the SD card in a file folder entitled "Steve File". The document appeared to contain a list of account names and passcodes. The list included the following:
 - i. Listed under the heading of "Amazon" was the email address riversidepresident2006@yahoo.com and an apparent passcode.
 - ii. Listed under the heading of "HauteLook" was the email address csikirby82@gmail.com and an apparent passcode.
 - iii. Listed under the heading of "Email" were the following email addresses: riversidepresident2006@yahoo.com, csikirby@gmail.com, and csikirby82@gmail.com.

Service of Additional Administrative Subpoenas and Search Warrant

103. On or around May 14, 2019, an administrative subpoena was served to Oath Holdings Inc. requesting subscriber information for the email account riversidepresident2006@yahoo.com (the email account listed on the transactional record located in the trunk of the SUBJECT VEHICLE), as well as a log of IP addresses utilized to access the account during the time period of April 23, 2018 through May 13, 2019. Records received in response to the subpoena provided the following information:
- a. The account was created on or around February 14, 2006 in the name of “S K” (which are KIRBY’s initials). The account was currently active.
 - b. The log of IP addresses identified that the account had been logged into on approximately 42 occasions during the approximate time period of May 25, 2018 through May 11, 2019 (one day after the execution of the search warrants at the SUBJECT PREMISES). The following were noted regarding the IP addresses utilized to log into the riversidepresident2006@yahoo.com account:
 - i. IP addresses serviced by Charter Communications were utilized to log into the account on approximately 28 occasions. These IP addresses included 74.140.165.102 (the IP address used to transmit messages for the yourmister2018 and yourmister2019 accounts and that is subscribed to Adult Female A at the SUBJECT PREMISES) as well as what appeared to be dynamic IP addresses.
 - ii. IP addresses serviced by Verizon’s cellular telephone network were utilized to log into the account on approximately eight occasions. The use of IP addresses associated with Verizon’s network is consistent with someone using the data plan of his/her cellular telephone to access the Internet – which is also consistent with the use of TARGET CELL PHONE-2 (which is serviced by Verizon).
 - iii. An IP address serviced by Comcast was utilized to log into the account on approximately one occasion.
 - iv. An IP address serviced by Leaseweb USA was utilized to log into the account on approximately one occasion.
 - v. An IP address serviced by Broadband Hospitality (a hotel provider) was utilized to log into the account on approximately one occasion.
 - vi. An IP address serviced by the Ohio Public Library Information Network (the same IP address utilized to transmit messages for the yourmister2019 Kik account) was utilized to log into the account on approximately three occasions. These three occasions were all on May 11, 2019 (the day after the execution of the search warrant).
104. On or around May 29, 2019, an FBI investigator served an administrative subpoena to Charter Communications requesting subscriber information for a sample of three of the dynamic IP

addresses utilized to log into the riversidepresident2006@yahoo.com account on a sample of the dates and times that they were utilized to access the account. Records received from Charter Communications in response to the subpoena identified that the three IP addresses were subscribed to Adult Female A at the SUBJECT PREMISES.

105. On or around April 16, 2019 and May 13, 2019, FBI investigators served administrative subpoenas to Apple Inc. requesting subscriber information and IP logs for any iCloud or other Apple accounts associated with the email address riversidepresident2006@gmail.com and telephone numbers 937-684-5792 and 937-304-8099. Records received from Apple Inc. in response to the subpoena provided the following information:
- a. An iCloud account associated with the Apple ID of riversidepresident2006@gmail.com and DSID of **188911353** was created on or around January 10, 2012. The account had an account name of "STEPHEN KIRBY", a mailing address of the SUBJECT PREMISES, and a customer telephone number of 937-684-5792 (the telephone number for TARGET CELL PHONE-2).
 - b. The "rescue" or recovery email for the account associated with the Apple ID of riversidepresident2006@yahoo.com was csikirby@gmail.com. Apple Inc.'s notes indicated that a representative from Apple Inc. had verified the csikirby@gmail.com email address.
 - c. The iCloud account noted above was presently associated with three devices: an Apple iPhone SE bearing serial number DX3W3ZVBHTVL (consistent with TARGET CELL PHONE-2 and the device seized from KIRBY's pocket pursuant to the search warrant), an Apple iPhone 7 Plus bearing serial number F2MSYHC0HFY1 (consistent with TARGET CELL PHONE-1 and the device seized from KIRBY's pocket pursuant to the search warrant), and an Apple watch bearing serial number FH7QM44MG9J6 (consistent with the watch seized from KIRBY's person pursuant to the search warrant).
 - d. The logs of IP addresses associated with the iCloud account identified that one or more of the associated devices was (were) backed up on a number of occasions. Based on the records, I have not been able to determine at this time if one or both of the iPhones were backed up to the iCloud account. The log included a total of approximately 2,159 entries of backup events. Below is a summary of the IP addresses utilized to conduct the backup events:
 - i. The IP address of 74.140.165.102 (which was utilized to transmit messages for the yourmister2018 and yourmister2019 Kik accounts and to log into the riversidepresident2006@yahoo.com email account, and that is subscribed to Adult Female A at the SUBJECT PREMISES) was utilized for the backup events on approximately 955 occasions.
 - ii. The IP address of 174.97.108.225 (which was utilized to transmit messages for the yourmister2018 Kik and yourmister2019 Kik accounts and that is subscribed to KIRBY at 3150 Charlotte Mill Road in Dayton, Ohio) was utilized for the backup events on approximately 51 occasions.

- iii. The IP address of 76.192.65.81 (which was utilized to transmit messages for the yourmister2019 Kik account and that is subscribed to Fitness International LLC, with a service address at the LA Fitness in Beavercreek Ohio) was utilized for the backup events on approximately 133 occasions.
 - iv. IP addresses serviced by Sprint's cellular telephone network (consistent with the use of TARGET CELL PHONE-1) were utilized for the backup events on approximately five occasions.
 - v. IP addresses associated with Verizon's cellular telephone network (consistent with the use of TARGET CELL PHONE-2) were utilized for the backup events on approximately 497 occasions.
 - vi. A number of other IP addresses were utilized to conduct the backup events on the approximately 518 remaining occasions. Some of these IP addresses appear to be potentially consistent with the use of a VPN.
106. On or around June 10, 2019, a search warrant was authorized by the United States District Court for the Southern District of Ohio for information associated with the email address riversidepresident2006@yahoo.com that is stored at premises controlled by Oath Holdings Inc. On or around July 9, 2019, Oath Holdings Inc. provided records in response to the search warrant. To-date, a preliminary review has been conducted of the contents of the email messages contained in the account. The following information was noted during the preliminary review:
- a. During the approximate time period of June 2018 through May 2019, approximately eleven email messages were received by the riversidepresident2006@yahoo.com account that were from an email address associated with the Google website. These email messages identified that the riversidepresident2006@yahoo.com account was the recovery email address for the following Google accounts: csikirby@gmail.com, csikirby82@gmail.com, and becauseiamawesome82@gmail.com. The email messages from Google informed the user of the riversidepresident2006@yahoo.com account about new activity related to the associated Google accounts, including the following:
 - i. Consistent with the email fragments recovered from the Dell All-in-One computer (as detailed in paragraph 101(f)), two emails were received on or around June 5, 2018 stating that a new Apple iPhone had been utilized to sign into the csikirby@gmail.com and csikirby82@gmail.com accounts.
 - ii. On or around June 11, 2018 and September 12, 2018, emails were received stating that a new Windows device was utilized to sign into the csikirby82@gmail.com account. On or around September 1, 2018, an email was received stating that the recovery phone for the csikirby82@gmail.com account had been changed.
 - iii. On or around June 22, 2018, an email was received stating that a new Tizen device (a Linux-based mobile operating system) had been used to sign into the

- csikirby@gmail.com account. On or around August 29, 2018, an email was received stating that a new Windows device was utilized to log into the csikirby@gmail.com account. On or around August 29, 2018, an email was received stating that a new Mac device was utilized to log into the csikirby@gmail.com account. On or around September 13, 2018, an email was received stating that the recovery phone had been changed for the csikirby@gmail.com account.
- iv. On or around July 3, 2018, an email was received stating that the recovery phone was changed for the becauseiamawesome82@gmail.com account. On or around February 25, 2019, an email was received stating that a new Windows device was utilized to sign into the becauseiamawesome82@gmail.com account.
 - 1. PO Owens has not authorized KIRBY to utilize the becauseiamawesome82@gmail.com account. As such, KIRBY is forbidden by the terms of his probation from utilizing this account.
 - v. On or around May 11, 2019 (one day after the execution of the search warrants at the SUBJECT PREMISES), two emails were received stating that a new Windows device was utilized to log into the csikirby@gmail.com and csikirby82@gmail.com accounts.
 - vi. On or around May 12, 2019 (two days after the execution of the search warrants at the SUBJECT PREMISE), two emails were received stating that a new Apple iPad was utilized to log into the csikirby@gmail.com and csikirby82@gmail.com accounts. Two additional emails were received stating that the passwords for the csikirby@gmail.com and csikirby82@gmail.com accounts had been changed.
 - vii. On or around May 16, 2019 (five days after the execution of the search warrants at the SUBJECT PREMISES), an email was received stating that a new Windows device was utilized to log into the csikirby@gmail.com account. On or around May 26, 2019 (sixteen days after the execution of the search warrants at the SUBJECT PREMISES), an email was received stating that a new iPad was utilized to log into the csikirby@gmail.com account.
- b. During the approximate time period of April 2019 through May 2019, approximately three email messages were received by the riversidepresident2006@yahoo.com account that were from an email address associated with the Yahoo website. These messages provided the riversidepresident2006@yahoo.com account user with notifications regarding its email account. These email messages included the following:
- i. On or around April 8, 2019, an email message was received stating that the alternate email address for the account had been changed to c*****by@gmail.com (intentionally masked by the sender, but consistent with csikirby@gmail.com).

- ii. On or around May 11, 2019, two email messages were received stating that the password for the riversidepresident2006@yahoo.com account had been changed and that a mobile telephone number ending in 07 had been removed from the account.
 - 1. TARGET CELL PHONE-1 and TARGET CELL PHONE-2 do not end in 07. As of this time, it is unknown what the referenced full telephone number is.
- c. At least approximately thirty-three email messages were received by the riversidepresident2006@yahoo.com account user that included KIRBY's name and/or address (the SUBJECT PREMISES).

Additional Interviews

107. As detailed above, an IP address subscribed to Adult Male B was utilized to transmit approximately 14 messages for the yourmister2019 Kik account (as detailed in paragraphs 81(b)(iv) and 83(a)). The approximately 14 messages were all transmitted on the same date in May 2019. On or around May 22, 2019, I interviewed Adult Male B. In summary, Adult Male B provided the following information:
- a. Adult Male B and KIRBY are friends, and they typically spent time together on a weekly basis.
 - b. Adult Male B was asked if he had any interaction with KIRBY on the date that the yourmister2019 Kik account utilized the IP address subscribed to Adult Male B. After reviewing text messages on his cellular telephone, Adult Male B identified that KIRBY likely came to a dinner party at Adult Male B's house that evening. Although Adult Male B did not recall ever telling KIRBY the password to the wireless Internet account at the residence, Adult Male B advised that one of his other friends at the party might have done so.
 - c. Adult Male B was only aware of KIRBY having one iPhone. Adult Male B had never used KIRBY's iPhone and did not know the password to unlock the device.
108. As detailed above, an IP address subscribed to KIRBY at 3150 Charlotte Mill Road in Dayton, Ohio was utilized to transmit approximately 12 messages for the yourmister2018 Kik account and approximately 20 messages for the yourmister2019 account (as detailed in paragraphs 80(b)(iii), 81(b)(iii), and 82(c)). Again as detailed above, Adult Female B (KIRBY's ex-wife) and her children currently reside at 3150 Charlotte Mill Road. On or around May 22, 2019, I interviewed Adult Female B. In summary, Adult Female B provided the following information:
- a. KIRBY had opened an Internet account in his name at Adult Female B's residence so that their children could utilize the Internet for school work. Adult Female B did not know if KIRBY knew the password to access the Internet service. She surmised that their children may have told KIRBY the password.

- b. KIRBY had regular supervised visitations with his and Adult Female B's children. Although the visitations were typically held at restaurants or shopping centers, KIRBY sometimes came to the house at 3150 Charlotte Mill Road.
 - c. Adult Female B was asked if she had any interaction with KIRBY on a sample of approximately four of the dates that the yourmister2018 and yourmister2019 Kik accounts utilized the IP address subscribed to KIRBY at her residence. After reviewing the text messages on her cellular telephone, Adult Female B advised that KIRBY was likely at her house on at least one of the dates.
 - d. Adult Female B was only aware of KIRBY having one iPhone. Adult Female B had never used KIRBY's iPhone and did not know the password to unlock the device.
 - e. KIRBY utilized the email address riversidepresident2006@yahoo.com.
109. On or around July 2, 2019, I interviewed Adult Female A. In summary, Adult Female A provided the following information:
- a. Adult Female A confirmed that KIRBY had lived with her since he was released from the custody of the Bureau of Prisons. No one else resided at the residence. Adult Female A confirmed that she had been in Florida from approximately late-January 2019 through mid-May 2019. As far as Adult Female A was aware, KIRBY lived alone at the house while she was in Florida.
 - b. A password was required to access the Internet account at Adult Female A's residence. Adult Female A had not shared the password with any of her neighbors or friends. Adult Female A was not aware of anyone else who used her Internet service.
 - c. The Dell All-in-One computer seized pursuant to the search warrant belonged to Adult Female A. Adult Female A's daughter occasionally used the computer. Otherwise, Adult Female A was not aware of anyone else who used the computer. Adult Female A had not shared the password to access the computer with KIRBY, and she had never seen him use the computer. However, Adult Female A suspected that KIRBY had utilized the computer to print documents on past occasions.
 - i. It should be noted that Adult Female A's daughter arrived at the conclusion of the interview. The daughter stated that one of Adult Female A's granddaughters had likely used the Dell All-in-One computer on past occasions.
 - d. Adult Female A had a flip-style LG cellular telephone. She had never used any of KIRBY's cellular telephones.
 - e. Adult Female A had limited knowledge of computers and computer applications. She did not utilize any email accounts or messenger applications, to include Kik Messenger, Telegram, and Omegle. She did not utilize any cloud storage services such as Dropbox and OneDrive.
 - f. Adult Female A did not know anyone who used the account names of mymister2018,

yourmister2018, and yourmister2019. Adult Female A did not know anyone who used the email addresses riversidepresident2006@yahoo.com, csikirby@gmail.com, and csikirby82@gmail.com.

- g. Adult Female A had not viewed pornography of any kind on her Dell All-in-One computer.
- h. Adult Female A was shown a photograph of the note that was affixed to the Dell All-in-One computer when it was seized (which contained “csikirby@gmail” and a possible password). Adult Female A did not recognize this note and advised that it did not contain her handwriting.
- i. While in Florida, Adult Female A obtained a new Apple iPad or tablet. She brought this iPad home with her when she returned to Ohio, and it was presently at the SUBJECT PREMISES. As detailed in paragraphs 106(a)(vi) and (vii), a new iPad was used to sign into the csikirby@gmail.com and csikirby82@gmail.com email accounts in May 2019, shortly after the execution of the search warrants.
 - i. Based on this and other information noted in the Affidavit, it is reasonable to believe that KIRBY may have utilized Adult Female A’s iPad to log into his email accounts.

Conclusions Regarding Use of Messenger Accounts and Devices

- 110. As detailed above in paragraph 75(b), Adult Male A identified that he exchanged iMessages with “Steve” via TARGET CELL PHONE-1, and that “Steve” utilized two Kik accounts: yourmister2018 and yourmister2019. Adult Male A also identified that “Steve” had a Telegram account. As noted above, Adult Male A identified “Steve” via a photographic lineup as KIRBY. As detailed above in paragraphs 78 through 82, records from Kik Interactive Inc. and Charter Communications indicate that KIRBY also utilized a Kik account with the account name of mymister2018.
- 111. It was noted that the activation date for TARGET CELL PHONE-1 (on or around November 8, 2018, as detailed in paragraph 87(a)) was after the date of the group chat reported by Kik Interactive Inc. (on or around June 8, 2018, as detailed in paragraph 69). As detailed above in paragraph 79(b), the records from Kik Interactive Inc. identified that the mymister2018 Kik account utilized Internet service associated with Verizon’s network on a number of occasions to transmit messages. This information is consistent with the utilization of TARGET CELL PHONE-2, which is serviced by Verizon.
- 112. As detailed above in paragraph 77(e), the yourmister2019 Kik account user identified that he was using a “public” phone at the time he was communicating with UCO-1 on or around April 18, 2019. Based on the information detailed in the Affidavit, this statement is indicative that the yourmister2019 account user was utilizing TARGET CELL PHONE-2 to communicate with and send a video file of child pornography to UCO-1. The yourmister2019 Kik account user indicated that he had another phone that had more child pornography files, and that he had access to more child pornography files at his residence. Based on this and other information noted in the Affidavit, it is reasonable to believe that KIRBY was referring to TARGET CELL

PHONE-1 when he mentioned his other telephone that contained child pornography files. Also based on this and other information noted in the Affidavit, it is reasonable to believe that the yourmister2019 Kik account user utilized two cellular telephones (TARGET CELL PHONE-1 and TARGET CELL PHONE-2) in furtherance of his child pornography activities.

113. As detailed above in paragraph 76, "Steve" indicated to Adult Male A that he had an application on his telephone that hid his files, and that he had the ability to "scrub" his telephone to remove files. Based on my training and experience, I know that child pornography offenders utilize various applications and techniques to hide their files. These applications and techniques can hinder law enforcement officers' ability to detect the files. Although PO Owens has not detected child pornography files on TARGET CELL PHONE-2, the comments made by "Steve" indicates that KIRBY utilizes one or more techniques to hide his files.
114. Based on all of the information detailed in the Affidavit, there is probable cause to believe that KIRBY is the user of the mymister2018, yourmister2018, and yourmister2019 Kik accounts; the yourmister2018 Telegram account; TARGET CELL PHONE-1; and TARGET CELL PHONE-2. There is also probable cause to believe that he has utilized the three Kik accounts, the Telegram account, and the two cellular telephones to possess, receive, and distribute child pornography and to discuss the sexual exploitation of children. Although KIRBY has denied using Adult Female A's Dell All-in-One computer, there is probable cause to believe that he has utilized this computer to access and view child pornography.
115. As detailed above in paragraph 100(j), KIRBY denied utilizing any email accounts other than sekirby2@gmail.com. As detailed above, KIRBY is prohibited by the terms of his probation from utilizing any other email accounts. Based on the records provided by Oath Holdings Inc. and Apple Inc. (as detailed in paragraphs 103, 105, and 106), the information provided by Adult Female B (as detailed in paragraph 108(e)), the data recovered from the Dell All-in-One computer (as detailed in paragraphs 101(a) through 101(k)), and other information detailed in the Affidavit, there is probable cause to believe that KIRBY has also utilized the riversidepresident2006@yahoo.com, csikirby@gmail.com, csikirby82@gmail.com, and becauseiamawesome82@gmail.com email accounts. It is reasonable to believe that KIRBY has continued to utilize these email accounts after the execution of the search warrant, contrary to the conditions of his supervised release.

Evidence Available in Email Accounts

116. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
117. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use

the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

118. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
119. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.
120. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone accounts that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
121. As detailed above, I know that email and other Electronic Service Providers often send messages to users' recovery email addresses regarding account activity associated with the users' linked accounts – such as the email messages described in paragraphs 106(a) and 106(b). These messages can help in identifying other computer devices and telephone numbers utilized by subjects in furtherance of their child pornography and child exploitation activities.
122. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.
123. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This

information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

124. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.
125. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
126. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

Evidence Sought in Searches of OneDrive Accounts

127. Based on the information recovered from the Dell All-in-One computer and other information detailed in the Affidavit, there is probable cause to believe that KIRBY has utilized one or more OneDrive accounts. There is also probable cause to believe that these OneDrive accounts are associated with one or more of KIRBY's email addresses – that being csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, sekirby2@gmail.com, and riversidepresident2006@yahoo.com.
128. OneDrive and other cloud storage services provide a means for individuals to store files. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
129. Based on my training and experience, I know that OneDrive and other cloud storage providers maintain basic subscriber information for its users, such as user names, email addresses, and the dates that they established their accounts. Such information can provide material evidence regarding individuals involved in child pornography offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.
130. As detailed above, Microsoft Corporation maintains various transaction information about the creation and use of the OneDrive accounts. Such information provides material evidence to

child pornography investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.

Conclusion Regarding Use of Email and OneDrive Accounts

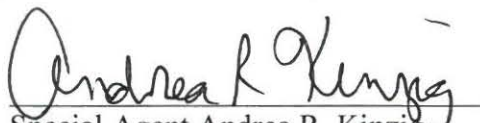
131. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts contains evidence of KIRBY's child pornography and child exploitation activities.
 - a. The Google accounts, csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, and sekirby2@gmail.com; and
 - b. OneDrive accounts associated with the email addresses csikirby@gmail.com, csikirby82@gmail.com, becauseiamawesome82@gmail.com, sekirby2@gmail.com, and riversidepresident2006@yahoo.com.
132. Preservation requests were served to Google LLC for the above noted accounts on or around May 23, 2019; July 1, 2019; and July 18, 2019. A preservation request was served to Microsoft Corporation for the above noted accounts on or around July 18, 2019.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

133. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google LLC and Microsoft Corporation to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

134. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; may be located in the accounts described in Attachments A-1 and A-2, including evidence of the following violations: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1).
135. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.
136. Because the warrants for the accounts described in Attachments A-1 and A-2 will be served on Google LLC and Microsoft Corporation, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 18th of July 2019


SHARON L. OVINGTON
UNITED STATES MAGISTRATE COURT JUDGE